North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

Quick Links

North Dakota

Too soon for flood outlook. Hard statistics to base any flooding estimates for this year are still unavailable for the Jamestown, North Dakota area. However, U.S. Army Corps of Engineers officials see a lot of early similarities to one year ago. "Plains snow pack amounts on Jan. 1, 2011 are similar to amounts monitored last year on Jan. 1," the Corps' senior public affairs specialist said in a press release. The 2010 high water event prompted releases from the Jamestown and Pipestem dams at 1,800 cubic feet per second. That level of release puts the James River in Jamestown at flood stage. In 2009, high water levels prompted releases of 3,200 cfs from the two dams. The National Oceanic and Atmospheric Administration estimates between 2 and 4 inches of snow water equivalent throughout North Dakota. Field testing done January 3 found the estimates were within 10 percent of actual moisture content. Snow water equivalent is the amount of moisture in the current snow if it is melted. This compares to estimates at the beginning of 2010 of 3 to 4 inches across the central parts of North and South Dakota. The National Weather Service (NWS) has not made any river or lake stage predictions for the Jamestown or Pipestem dams. The NWS does forecast a 10 percent chance of major flooding on the Pipestem at Pingree and a 2 percent chance of major flooding on the James River at LaMoure. "Based on the current numbers and the extended forecast we could be seeing something similar to last year," the county emergency manager said. "But the first hard numbers will come in during the early- to middle part of February." Source: http://www.jamestownsun.com/event/article/id/126828/

Man makes bomb threat at Mandan grocery store. Police in Mandan, North Dakota, are looking for a man who threatened to set off a bomb at a supermarket unless he was given drugs. A police lieutenant said at about 5 p.m. December 31, a man wearing a ski mask walked up to the pharmacy at the Dan's Supermarket on 500 Burlington St. S.E. and gave employees a note asking for a specific drug or else he would detonate a bomb. Store workers did not give him anything, and he left the store. No explosives were found. Source: http://www.bismarcktribune.com/news/local/article_87d1d660-16a9-11e0-912c-001cc4c03286.html

Regional

(Minnesota) **Officials warn of tainted apple cider.** Officials in Minnesota have urged people not to drink certain types of apple cider made by the Pepin Heights Orchard. Lab tests found that it might have patulin, a mold toxin. The company is located at Lake City on the Minnesota-Wisconsin border. And the cider in question was sold in half-gallon and one-gallon plastic jugs in Wisconsin, Minnesota, Iowa, Florida, Texas, and Arizona. No one has been reported to get sick from drinking the cider. Officials said consumers should discard it. Meanwhile, the orchard is working with Minnesota agriculture officials to find the source of the toxin. Source: http://whbl.com/news/articles/2010/dec/31/officials-warn-tainted-apple-cider/

(Minnesota) **Cyber crime trail leads to Winona State students.** A U.S. Department of Homeland Security investigation dubbed "Operation eMule" has led federal agents to a pair of 22-year-old foreign-exchange students in Winona, Minnesota, who are suspected to be part of a sophisticated cyber crime ring based in Vietnam that has been misusing the identities of countless Americans to bilk online retailers out of millions of dollars. Numerous major companies have been stung in the scam, including eBay, PayPal, Amazon, Apple, Dell, and Verizon Wireless, according to federal court documents. Authorities said the operation is built around stolen identities used to open accounts with eBay, PayPal, and U.S. banks. Through those accounts, the fraudsters sell popular, expensive merchandise at discounted prices. The sellers fill the orders by purchasing the goods from other vendors using stolen financial accounts. When the identity-theft victims protest the charges, the merchants end up holding the bag. The two Winona State University students controlled more than 180 eBay accounts and more than 360 PayPal accounts opened using stolen identities, according to documents unsealed December 29 by a federal magistrate judge in St. Paul. Source: http://www.startribune.com/local/112754219.html?elr=KArks7PYDiaK7DU2EkP7K_V_GD7EaPc:iLP8iUiD3aPc:_Yyc:aU7DYaGEP7vDEh7P:DiUs

National

BP oil spill IT systems lacked key alarms. BP's monitoring IT systems on the failed Deepwater Horizon oil rig relied too heavily on engineers following complex data for long periods of time, instead of providing automatic warning alerts. That is a key verdict of the Oil Spill Commission (OSC), the authority tasked by the U.S. President to investigate the Gulf of Mexico disaster. It also criticized decisions to ignore cement modeling tests, as well as other cementing and management strategies. The OSC said in a chapter released January 6 that the monitoring systems on the rig before the explosion provided the necessary safety data, including about pressure in the well. However the systems relied too much on engineers' astute manual observation of data flows. It also noted the systems used by BP were standard in the energy industry. When engineers were tasked with so many simultaneous functions over long work days, they needed much more support from systems. The standard industry ones used by BP were too basic, the OSC said. In a chapter of the report, panelists expressed exasperation that while the industry was regularly conducting highly complex drills in order to satisfy the global demand for oil, IT systems simply have not kept pace with the complications and risks of deepwater drilling. The full report will be published next week. Source: http://www.computerworld.com/s/article/9203749/BP_oil_spill_IT_systems_lacked_key_alarms

(Texas) **Two suspects in oil products heist at large.** Law officers in Montague County, Texas are attempting to arrest more people indicted in connection with the theft of more than $1 million in petroleum products. In a Montague County grand jury session, 23 sealed felony indictments for theft, engaging in organized criminal activity, and conspiracy were issued against seven individuals, said the district attorney. These indictments bring the total to 10 people charged in connection with two-and-a-half year investigation by the Texas Rangers, Montague County DA's office, and the Wise County Sheriff's Office. An investigator with the Wise County Sheriff's Office, said the December indictments were for charges of theft, money laundering, engaging in organized criminal activity, and conspiracy. A spokesman said the thieves used various methods to steal the oil, but the most common was for saltwater truck drivers to go to clandestine sites and change out the water for oil. They also would get half a load of water and half a load of oil. The stolen oil was then sold at less than half price to companies in Montague County. Another method would have the drivers obtain keys to trucks from

deserted businesses at night and take them to steal the oil. Source: http://www.timesrecordnews.com/news/2011/jan/06/two-suspects-in-oil-products-heist-at-large-n-of/

INTERNATIONAL

Hijacker overpowered on Norway-Turkey flight. Passengers aboard a Turkish Airlines flight from Oslo, Norway, overpowered a would-be hijacker as the plane landed at an Istanbul, Turkey airport January 5, fellow passengers told Turkish media. Police said the man was a Turk who had demanded the plane return to Norway. His motive was unclear. According to the Turkish Dogan news agency, he tried to force his way into the cockpit of the plane saying: "I have a bomb." The pilot notified emergency services at Istanbul's Ataturk International Airport. Passengers were taken off after landing and the man was arrested, and the bomb found to be a fake. Police said a passenger was sitting on the hijacker when they entered the plane, a Dogan journalist reported. Private Norwegian television network TV2 quoted a witness as saying someone in the back of the plane put on a mask and threatened to blow up the plane in the air. He said the crew moved the other passengers to the front of the plane, while the hijacker remained at the back. There were no reports of injuries. Source: http://www.nytimes.com/reuters/2011/01/05/world/international-uk-turkey-norway-hijack.html?_r=1&ref=world

Australian flooding 'to last weeks'. Devastating flood waters across the Australian state of Queensland may not recede for weeks, the state's premier has warned. More than 20 towns in Queensland have been cut off or flooded, with more than 200,000 people affected. Military aircraft are flying supplies into Rockhampton, which was isolated by the still-rising waters. People were being ordered by police to leave their homes. They were wading through outlying suburbs, chest-deep at times, to tell people to leave. Many were reluctant to do so. There have been reports of small-scale looting and many people were worried not just by the floodwaters, but by the possibility their homes might be robbed. That is why an evacuation center which has room for 1,500 people, had only 50 overnight January 2 into January 3. The extent of flooding being experienced by Queensland is unprecedented and requires a national and united response, officials said. Approximately 850,000 square kilometers have been affected, an area equivalent in size to France and Germany. Source: http://www.bbc.co.uk/news/world-asia-pacific-12107131

New year mobile bug strikes French texters. Hundreds of French mobile phone users said a bug prompted them to send dozens of unintended new year messages. French mobile operators have already revealed that 930 million texts were sent on New Year's Eve (December 31) and New Year's Day (January 1). Now it has emerged that individual Orange customers unwittingly sent as many as 130 text or picture messages — potentially at a high extra cost. Orange has blamed a "network operator failure" for the bug, saying it affected only a few hundred people. Dozens of customers complained the problem led to them being charged hundreds of euros extra. Multimedia (MMS) messages tend to be charged at a higher rate than text only (SMS) messages. One user wrote on an Orange user forum that he had been billed for 300 picture messages. Another complained his family and friends had received the same MMS text 15 times. Orange, which is owned by France Telecom, pledged that no-one would be overcharged. A spokesman for the company said that one "of the network operators had had technical problems during the night" and refused to name the operator in

question. However, other operators insisted they had not encountered any difficulties. Source: http://www.bbc.co.uk/news/world-europe-12107920

Mexico finds 4 more illegal pipeline taps. Mexico's state-owned oil company said it found four more illegal taps drilled into pipelines by fuel thieves December 30. Petroleos Mexicanos said none of the taps caused leaks or spills. Two of the improvised taps were found in a gasoline pipeline in the northern state of Sinaloa. Another tap was found in the Gulf coast state of Veracruz. A fourth tap was found in the north-central state of Guanajuato, when police noticed a tanker truck filled with diesel sitting in a field. The December 30 announcement came after a December 19 explosion at a pipeline killed 29 people. Pemex officials said that explosion was apparently caused by an illegal tap. Pemex suffered more than 614 thefts from pipelines in 2010. Source: http://www.bloomberg.com/news/2010-12-30/mexico-finds-4-more-illegal-pipeline-taps.html

Banking and Finance Industry

600 credit-card numbers stolen at gas pump. Six hundred credit-card numbers were stolen at a Florida gasoline station by an operation that used a credit-card skimmer hidden inside a gas pump, police said. The skimmer, placed at a RaceTrac Petroleum Inc. gas station in Melbourne, Florida, by unknown thieves, recorded customers' credit-card information every time they swiped their cards to pay for gas, police said January 6. The allegedly stolen data led to complaints of fraudulent credit and debit card charges, police said. "We've had about 20 incidents that have been reported involving this particular gas station," a Melbourne police spokesman told Florida Today. Many of the stolen card numbers were used for purchases in New York City, mostly at a credit union, police said. Police have made no arrests, but "we do have a lead detective working on the case right now," the spokesman told the newspaper. Source: http://www.upi.com/Top_News/US/2011/01/06/600-credit-card-numbers-stolen-at-gas-pump/UPI-54631294358121/

Visa claims new software catches more fraud. Credit card companies choose to scrutinize some bits of information for signs of fraud while ignoring others. And those decisions are made in a fraction of a second when approving or denying a sale. Visa, which operates the world's biggest electronic payment network, spoke publicly January 6 for the first time about new technologies it put in place ahead of the 2010 holidays. The company said the upgraded systems can catch more fraud because its developers figured out ways for the software to look for more signs of bad behavior at once. Some of the variables include the speed of transactions on a particular card, the time of day, the physical distance between transactions, and the type of store. The new software, which rolled out in September, can combine more than a dozen different variables. That is important because the ability to sift through more data increases the odds of catching a fraudulent purchase before it is approved. Visa said upgraded software will allow Visa to spot a greater percentage of fraud. Detection of cross-border fraud, which Visa said it looked at intently for the latest iteration, shows major gains. Source: http://news.yahoo.com/s/ap/20110106/ap_on_hi_te/us_tec_techbit_visa_fraud_upgrade

Undetectable fake ATM keyboard steals PINs in real time. Thieves and scammers are an inventive bunch, especially when it comes to stealing money indirectly. And the latest discovery of a fake keyboard placed over an ATM's legitimate one that records the typed-in PIN — in conjunction with a fake magnetic strip reader that can be manufactured from cheap spare electronic parts — shows this kind of crime does not require a lot of funds and can bring in quite a lot of money. According to

Gizmodo, the keyboard is virtually undetectable by anyone who is not an expert, and looks exactly like the real thing. It records the PIN as you type it in and sends this information, and that regarding the credit card magnetic strip, to the criminals in real time, so they can immediately proceed to empty an account. U.S. ATM users are particularly susceptible to these types of theft, since many ATMs work on the same principle. The chip-and-PIN technology used in Europe is harder to crack, so a number of U.S. banks have started adopting it. Source: http://www.net-security.org/secworld.php?id=10402

AOL customers targeted in new phishing attack. A new phishing attack is targeting AOL subscribers by claiming that they need to update their account billing information in order to avoid facing restrictions. The rogue emails have their header spoofed to appear as originating from —AOL Member Billing Services and bear a subject of —Billing update on file must be performedz. The body uses an AOL template which includes an AOL Member Services banner and the enclosed message reads: —Our records indicate that your account hasn't been updated as a part of our regular account maintenance. Our new SSL servers check each account for activity and your information has been randomly chosen for verification. AOL Member Services strives to serve their customers with better and secure banking service. Notification: Failure to update your account information may result in account limitation at shopping on our portal. A link called —Update your information is included and, if clicked, takes recipients to a phishing page which displays a form for inputting a wealth of information. This includes name, address, city, state, zip code, country, phone number, birth date, Social Security number, driver's license number, as well as credit card type, number, CVV2, PIN, expiration date, issuing bank, bank routing number, and bank check account. Information about the AOL account itself, such as screen name, password, security question, and answer are also required. Source: http://news.softpedia.com/news/AOL-Members-Targeted-in-New-Phishing-Attack-176351.shtml

The evolution of cyber criminal operations. There is a concerning evolutionary step cyber criminal operations are taking to more effectively diversify the distribution of their ill-gotten gains, according to Fortinet. The campaigns, which were seeded in a number of Asian and European countries, solicited local individuals who already have or had established relationships in the banking industry or were looking for work as _online sales administrators'. To make these —localized campaigns even more effective, they incorporated regional-sounding domain names, such as cv-eur.com, asia-sitezen.com, and australia-resume.com. Upon closer scrutiny, Fortinet discovered all three domains were registered to the same Russian contact, and all contact addresses for worldwide recruitment used Google mail hosting. By using localized campaigns, criminals can obtain mule accounts internationally – each one falling under different banks and governing laws. Thus, if one is taken offline (due to increased enforcement activity), the others will remain online and business will be as usual. Cleverly engineered spam mail with malicious attachments/intentions can be much more damaging than non-effective spam by the masses. Source: http://www.net-security.org/secworld.php?id=10391

The evolution of check fraud. Despite an overall, albeit gradual, decline in check use, check fraud continues to plague the financial industry. And banks and credit unions are challenged to curb these evolving crimes. According to the new Faces of Fraud Survey, check fraud is one of the top three fraud forms plaguing banking institutions, joining the likes of phishing and vishing, and payment card fraud. Sixty-three percent of survey respondents say they experienced check fraud in 2010. Yet only

34 percent of banks and credit unions say they are well equipped to fight these crimes. —Check fraud is so prevalent because it's easy, said the vice president of the Center for Regulatory Compliance within the Financial Policy and Regulatory Affairs division of the American Bankers Association. —This is low-tech crime, and a lot of fraud prevention in this area is focused on training frontline tellers to ask questions. ... When human interaction is involved, the human analysis is your best line of defense. Source: http://www.bankinfosecurity.com/articles.php?art_id=3231

FBI: Organized retail crime costs U.S. $30B a year. According to an article published the week of January 3 by the FBI, organized retail crime, which includes merchandise theft, as well as credit card fraud, gift card fraud, and price tag switching, costs the United States about $30 billion per year. The agency said the stores targeted by perpetrators of organized retail crime range from small specialty shops to major department stores. The groups responsible for these crimes include South American theft groups, Mexican criminal groups, as well as Cuban criminal groups from South Florida, and Asian street gangs from California. A Special Agent of the FBI's Violent Crimes/Major Offenders Unit in Washington, D.C. called organized retail crime a "gateway crime" often used to fund other criminal endeavors. The FBI said it is working with the retail industry to help address the problem, and noted it recently helped to develop the Law Enforcement Retail Partnership Network (LERPnet), which is a database that can be used by retailers to report and share incidents of retail theft and other retail crimes. Source: http://www.securityinfowatch.com/fbi-organized-retail-crime-costs-us-30b-a-year

Top 9 security threats of 2011. Mobile banking and social networks are expected to pose new security threats in the payments space in 2011. But security experts said those threats would not displace the Zeus botnet, malware attacks, and phishing threats, which for years have plagued banking institutions. Fraud attempts will escalate, not diminish, as new threats and channels blossom in 2011. As 2010 came to a close, Information Security Media Group caught up with a handful of leading industry experts to get their takes on the top security threats of 2011. The top 9 threats of 2011 include:(1) Mobile Banking Risks, (2) Social Networking Risks, (3) Malware, Botnets, and DDoS attacks, (4) Phising, (5) ACH Fraud that leads to Corporate Account takeovers, (6) Cloud Computing Risks, (7) Insider Threats, (8) First Party Fraud, and (9) Skimming Attacks. Source: http://www.bankinfosecurity.com/articles.php?art_id=3228

Chemical and Hazardous Materials Sector

Homeland Security delivers nuclear detection plan to Capitol Hill. A key U.S. Homeland Security Department agency recently submitted to lawmakers the blueprint for the federal government's effort to prevent nuclear-weapon materials from being smuggled into the country. The Domestic Nuclear Detection Office (DNDO) delivered its long-awaited "strategic plan" for the global nuclear detection architecture to Capitol Hill December 20, according to the DNDO chief. The Homeland Security Secretary signed off on the plan that same day. The detection architecture usually refers to the worldwide network of sensors, telecommunications, personnel, and measures used to detect, identify, and report the potential movement of illicit nuclear and radioactive materials or weapons. The blueprint, which has yet to be made available to the public, details the detection office's vision for the system over the next 5 years as well as the objectives and performance metrics for the architecture, the DNDO chief said. Source: http://www.globalsecuritynewswire.org/gsn/nw_20110105_2909.php

U.S. revises hazmat transport special permits procedure. The U.S. Pipeline and Hazardous Materials Safety Administration has issued a final rule revising its procedures for applying for special permits to transport hazardous materials in commerce. The new procedures mandate that applicants offer sufficient information to ensure the agency is able to evaluate their ability to undertake the activities of the special permit, clarify current requirements, and call for supplemental information to allow the agency to have better oversight. They also make an online application available. The changes will go into effect March 7. Source: http://rotor.com/Default.aspx?TabId=177&newsid375=72429

U.S. nuclear plant security concerns persist. Staged assaults of U.S. atomic energy plants by counterterrorism professionals in recent years have revealed security weaknesses that could be exploited by terrorists in an attack aimed at releasing stored radioactive material into the surrounding area, Newsweek magazine reported January 4. All 104 of the nation's atomic energy installations are faced every three years with mock terrorist attacks intended to help the sites assess potential security vulnerabilities. The drills are planned with care and facility chiefs receive 60 days advance notice to ready their security personnel. The attackers follow a choreographed plan of infiltration. Even with all of this advance information, since 2005 nearly 10 percent of the fake attack teams were able to cut through plants' security efforts, according to Newsweek. In a 2009 drill, trainers posing as extremists armed with automatic weaponry and grenade launchers were able to infiltrate an atomic energy site in the South by cutting through the barbed wire and chain-link barriers. The attackers fought with plant security personnel. Survivors from the assault force disrupted a key part of the reactor's operating machinery, which threatened in the scenario to produce a reactor core meltdown and the dispersal of radioactive material stored at the facility. Spent atomic fuel — comprised of plutonium, uranium and some other chemicals and formed into small pellets — is generally stored on-site at plants within cement containers in large pools of water. The material essentially constitutes a massive radiological —dirty bomb that could be released to the surrounding area if the water is drained away from the containers. U.S. regulators say that these successful staged attacks highlight reactor vulnerabilities that need to be addressed. The NRC says federal monitors stay at a plant until its weaknesses have been eliminated. Specifics about the defenses and weaknesses of U.S. plants are kept secret. Source: http://www.globalsecuritynewswire.org/gsn/nw_20110105_2790.php

EPA to require safety testing of 19 widely used chemicals. The Environmental Protection Agency (EPA) said January 4 new federal rules will require makers or importers of 19 chemicals to test the health and environmental effects of the substances and make the information public. The chemicals include diphenylmethanone; 9, 10-anthracenedione; C12-C24 chloroalkenes; pentaerythritol tetranitrate, or PETN; and leuco sulfur black. The American Chemistry Council, an industry group, supports the action as an extension of an existing EPA program in which chemical makers have been voluntarily reporting health and environmental effects of heavily used chemicals, said a spokesman. The 19 chemicals are among more than 2,200 chemicals produced or imported in the U.S. in large volumes every year. In recent years, the EPA has asked chemical makers and importers to voluntarily provide information to the public on health and environmental effects of potentially toxic chemicals that they make or import in quantities of one million pounds a year or more. Source: http://www.foxbusiness.com/markets/2011/01/04/epa-require-safety-testing-widely-used-chemicals/

U.S. nuclear output is little changed after Indian Point slows. U.S. nuclear-power production was little changed January 4 after Entergy Corp. slowed a unit at its Indian Point plant in Buchanan, New York, the Nuclear Regulatory Commission (NRC) reported. Production from U.S. reactors dropped by 144 megawatts from January 3 to 97,048 megawatts, or 96 percent of capacity, according to the NRC report and data compiled by Bloomberg. Four of 104 power units were offline. Entergy reduced power at its 1,020-megawatt Indian Point 2 reactor to 77 percent of capacity from 90 percent January 3. Source: http://www.bloomberg.com/news/2011-01-04/u-s-nuclear-output-is-little-changed-after-indian-point-slows.html

Commercial Facilities

(Arizona) **Chandler mall evacuated after suspect shoots at officers.** Chandler Fashion Center in Chandler, Arizona was evacuated and was on lockdown for several hours January 5 after a suspect fired shots at officers outside then ran into the mall. According to a Chandler police sergeant, an armed robbery occurred off the mall premises and the suspect went to the mall located at Chandler Boulevard and Loop 101 around noon. Undercover officers with the U.S. Marshals Task Force who were in the area pursued the suspect, who police identified as a 27-year-old man, and confronted him outside the mall. The sergeant said shots were exchanged, but no one was injured. The suspect then fled into the mall. The mall was placed on lockdown and people were evacuated while officers searched for him. Somehow the suspect was able to exit the mall. At approximately 12:30 p.m. there was a report of shots fired and a hostage situation inside a Baja Fresh restaurant north of the mall. Contact was made with the suspect and after about 1 hour of negotiations, he was taken into custody inside the Baja Fresh shortly before 3 p.m. without incident. Around 5 p.m., Chandler police confirmed the man was the original suspect from the shooting, and that the two incidents were related. Source: http://www.azfamily.com/news/local/Chandler-Fashion-Center-evacuated-for-suspect-search-112954299.html

(Florida) **Device rendered safe at West Melbourne office building.** A situation at a West Melbourne, Florida office has ended after the building was evacuated because of a suspicious device January 4. —The device was rendered safe, said a commander of the West Melbourne Police Department. The —hoax device was thought to have specifically targeted a law office around 2:30 p.m. All personnel had been evacuated from the State Farm Building at 2815 West New Haven Ave and the nearby Sun Trust Bank, which is across from Target in the Home Depot shopping plaza. The Brevard County Sheriff's Office explosive ordnance disposal team arrived just before 3:30 p.m., and the bomb squad ended the situation by 4:00 p.m. when they determined the device was a fake. Source: http://www.floridatoday.com/article/20110104/BREAKINGNEWS/110104014/1006/NEWS01/Device+rendered+safe+at+West+Melbourne+office+building

High alert for Coptic Christmas in Canada after terrorist attack in Egypt. Security has been increased at Coptic churches across Canada as they prepare to celebrate the birth of Christ this January 7, in the wake of a deadly terrorist attack in Alexandria, Egypt, January 1. Coptic Orthodox leaders in Canada have been contacted by the Royal Canadian Mounted Police (RCMP) due to concerns that extremists may target the Coptic diaspora abroad. The Head of the Canadian Coptic Association based in Montreal said the RCMP are taking every precaution to ensure no attacks are carried out as they celebrate the Orthodox Christmas. Officials said January 4 the attack in Egypt left at least 23 dead, and it sparked riots in Egypt and alarm across Europe and North America. Canada is believed to be

home to the largest Coptic diaspora after the United States, with conservative estimates at nearly 250,000, mostly living in Eastern Canada. There are five Coptic Orthodox Churches in Montreal and more than 20 in the Greater Toronto Area. The Canadian Press reported last month on an al-Qaeda website, Shumukh al Islam, that has a list of more than 100 Copts living in Canada and others around the world. Source: http://www.winnipegfreepress.com/canada/breakingnews/high-alert-for-coptic-christmas-in-canada-after-terrorist-attack-in-egypt-112889484.html

(Michigan) **Pipe under scrutiny in Mich. store explosion.** A federal agency will inspect a piece of natural gas pipe as regulators investigate an explosion that killed two people at a Detroit-area furniture store. A spokesman from the Michigan Public Service Commission told the Detroit Free Press January 1 that the pipe has been shipped to Houston, Texas for evaluation. Consumers Energy said it received two calls about a smell of gas December 29 before an explosion destroyed the William C. Franks Furniture store in Wayne, Michigan. The owner was rescued, but two employees were killed. The spokesman said the commission is checking whether the area has a history of natural gas leaks and whether the utility complied with regulations. Businesses were reopened December 31 except for ones that were connected to the furniture store or close to it. Source: http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102075.html

Communications Sector

Jam prisoners' cellphone calls? New federal report explores possibilities. The Presidential Administration does not want dangerous prison inmates to make calls or send text messages from contraband cellphones because of the possibility they could direct new crimes. But federal officials also do not want to go so far in trying to jam those communications that they create problems for nearby public safety workers or average citizens, according to a new government report. A possible solution: more limited technologies that would let prison officials block calls only from unapproved devices, the report said. In late 2009, Congress directed government officials — including the Federal Communications Commission, the Federal Bureau of Prisons, and the National Telecommunications and Information Administration — to look into technologies that could prevent the use of cellphones by inmates. A law enacted in August bans cellphones from federal prisons, but it does not apply to state facilities. In California state prisons, for example, inmates are not supposed to have cellphones, but there is no law that makes possessing one a crime, or that imposes penalties on visitors who smuggle them in. This year, California will test one technology, called managed access, with which officials can block calls that do not come from a list of phones approved to transmit through nearby towers. The system enabled Mississippi state officials to block more than 216,000 unauthorized calls and text messages in its first month in operation last summer. Source: http://latimesblogs.latimes.com/technology/2011/01/prison-cellphone-charles-manson-jam-government-fcc-report.html

Hackers breach Motorola phones. Researchers at the Chaos Computer Club Congress (CCC) in Berlin, Germany demonstrated a relatively easy hack of a Motorola mobile device by acquiring its ID and grabbing text and voice messages as they pass between a handset and a base station. The researchers' work builds on earlier research that found holes in many parts of GSM technology, the most widely used in the world today. The pair spent a year putting together the various parts of their simple system. Much of the capabilities are not new, but the clincher was the ability to record data

off the air, as well as the fact that the inexpensive Motorola phones can have their onboard software swapped for an open source alternative. This was made possible when a description of the firmware leaked to the Internet. Source: http://www.tele-management.ca/content/23539-hackers_breach_motorola_phones

Critical Manufacturing

(Indiana) **Mysterious package caused partial plant evacuation at GM.** A suspicious looking package had security at the GM automobile plant in Fort Wayne, Indiana, on high alert January 3. An unidentified pipe package with caps on each end arrived at the body shop entrance around 1:30 p.m. causing plant security to enact evacuation protocol for part of the plant along with a quarantine of the area. Local authorities were called in and after inspection, the contents of the package were found to be empty. Operations have resumed at the plant. Source: http://www.indianasnewscenter.com/news/local/Mysterious-Package-Caused-Partial-Plant-Evacuation-At-GM-112821349.html

Ford, Chrysler recalling thousands of vehicles. Ford Motor Co. is recalling 19,600 2011 model year trucks and crossover SUVs over concerns an electrical short could cause a fire, the manufacturer said December 30. Chrysler Group LLC also is recalling nearly 145,000 trucks and crossover wagons in three separate campaigns for steering, stalling, and airbag concerns, according to letters posted the week of December 26 on the Web site of the National Highway Traffic Safety Administration (NHTSA). Ford decided to recall certain 2011 model year F-150 trucks, Super Duty trucks (F-250 through F-550), and its Edge and Lincoln MKX vehicles after fires started in the cabs of two F-150 trucks at a Michigan assembly plant in November and December, the company said in a letter December 27 to the NHTSA. Ford said it will send recall letters to vehicle owners the week of January 10. Chrysler's recalls include one for 22,274, 2008-2011 Dodge Ram 4500 and 5500 trucks, with the manufacturer saying a ball stud at the end of a tie rod could fracture and lead to a loss of steering. The recall was announced after 86 consumer reports of tie rod replacements due to such a fracture. Also recalled are 65,180, 2009 Dodge Journey crossover wagons manufactured between November 1, 2007, and September 7, 2008, because side airbags may not deploy in a crash. Chrysler said side-impact pressure sensor circuits may be at risk of fatigue and breaking — a condition noticed after consumers reported they were seeing their airbag warning lamps light up. A third Chrysler recall involves 56,611, 2011 Dodge Ram 1500 trucks because of a rear axle bearing that could seize and cause the vehicle to stall, according to Chrysler. The manufacturer said it received 20 reports alleging axle-bearing noise or failure, and that most of the failures happened within 500 miles of driving. Chrysler's recalls are expected to begin in February, according to the NHTSA.Source: http://www.cnn.com/2010/US/12/30/ford.chrysler.recalls/index.html?iref=allsearch

Defense/ Industry Base Sector

Navy intel chief: Chinese missile is effective. The U.S. Navy's intelligence director said January 5 that officials were surprised by China's rapid development of a ballistic missile thought capable of striking ships at sea. "Their anti-ship missile — we underestimated when they would be competent and capable in delivering a technological weapon of that type," said the vice admiral, the deputy chief of naval operations for information dominance and the Navy's intelligence director. He was referring to development and testing of the Dong Feng 21D, a land-based anti-ship ballistic missile that officials

now say has reached its initial operating capability. Analysts said the missile leaves U.S. aircraft carriers vulnerable to attack, as the technology the missile utilizes increases its probability of being able to hit a moving target. Source: http://www.militarytimes.com/news/2011/01/navy-intelligence-chief-chinese-missile-is-effective-010511w/

DOD report says spying focused on naval technology. The U.S. Department of Defense in a new report covering espionage for 2009 said that attempts by foreign spies to obtain classified or restricted U.S. technology increased and that foreign governments are focusing their spying efforts on naval and marine technology that could provide the foundation for a next generation —blue water navy. The revelation comes in the 2010 edition of —Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry, an annual publication by the Defense Security Services, part of the U.S. Department of Defense. The report concludes that Internet based spying and targeted attacks from what the report refers to as —entities from —East Asia and the Pacific region continued to be a major problem for the U.S. military and military contractors. Source: http://threatpost.com/en_us/blogs/dod-report-says-spying-focused-naval-technology-010411

More cracks found on space shuttle Discovery's fuel tank. NASA revealed December 30 technicians have uncovered even more cracks on the space shuttle Discovery's external tank. It is unclear what effect these cracks will have on the shuttle's planned February 3 launch. Separate cracks prompted NASA to scrap a December 17 launch and push it to February. Since then, technicians have been working to fix the cracks and discover what caused them in the first place. With the latest round of X-ray image scans, technicians discovered small cranks on the top of stringers on panel 6, which is on the opposite side of the tank from the shuttle. Space Shuttle Program managers are meeting December 30 to decide if modifications on the stringers are needed. If they are, those modifications would begin January 3. Discovery was initially scheduled to take off and head to the International Space Station November 1. Leaks, inclement weather, electrical issues, and cracks, however, have delayed that launch more than a half dozen times. Source: http://www.pcmag.com/article2/0,2817,2374936,00.asp

Emergency Services

(Indiana) **Police investigating theft of copper wire in Decatur Co.** Indiana State Police are investigating the theft of thousands of dollars worth of copper from an Indiana State Police radio tower site in Decatur County. Three copper grounding bars and 10 feet of copper wire, valued at $6,000 to $10,000, were stolen between December 17 and January 6 from the site on Southwest Road 60. Source: http://www.therepublic.com/view/local_story/Police_investing_theft_of_copp_1294410458/

USFA: 2010 record low for on-duty deaths. Last year was record-setting — the fewest on-duty deaths of firefighters since the United States Fire Administration started compiling statistics in 1977. There were 85 on-duty deaths in 2010, according to preliminary statistics. Of those, 15 are classified as Hometown Heroes. In 2003, federal legislation was adopted that firefighters who died of heart attacks or strokes within 24 hours of a response or training receive that designation. This is the second year in a row that on-duty deaths showed a decline. In 2009, the country experienced the lowest number in 15 years. Of those who died in 2010, 55 were volunteers, 28 were career, one was a paid full-time wildland firefighter, and one was a paid-on call firefighter. Heart attacks continue to

claim the most firefighters — 56.4 percent — while trauma was reported in 23.5 percent of the deaths. Other causes included stroke, burns, heat exhaustion, asphyxiation, and crushing. Source: http://www.firehouse.com/news/top-headlines/usfa-2010-record-low-duty-firefighter-deaths

Plain language key to public safety communications. Law enforcement executives across the United States must commit to a plan and develop a road map that outlines the necessary steps to comply with The Department of Homeland Security policy initiative to migrate from older —Ten Code public safety radio systems to the use of —plain language in the National Incident Management System, according to a report released by the National Institute of Justice. The report, Law Enforcement Agencies Are Phasing Out Old Radio Codes, outlines several essential ingredients of such a road map. The need to communicate with other departments has grown in recent years, and the use of 10-codes — which vary across jurisdictions — can potentially confuse first responders from different agencies when they work together. To address this problem law enforcement must begin to standardize existing plain language terms. For instance, —Stolen car may be referred to as a GLA (grand larceny auto), a GTA (grand theft auto), or some other term in adjacent jurisdicÂtions. Plain language is encouraged by the Department of Homeland Security, the Association of Public-Safety Communications Officials, and the International Association of Chiefs of Police. Source: http://www.hstoday.us/briefings/daily-news-briefings/single-article/plain-language-key-to-public-safety-communications/5c47aa5aa646017b7109c268c322082f.html

(Texas) **Police recover blasting caps, and TNT, but not C4.** Corpus Christi, Texas police have recovered most of the explosives that were stolen from a police storage site in Annaville, Texas, December 8. Acting on a tip, police arrested a 20-year-old suspect, December 30, and found much of what they were looking for in the Nueces River near Labonte Park. As of January 3, police had recovered all 87 of the blasting caps, and TNT that was stolen, but had not recovered the C4 that was stolen. Dive teams recovered most of the stolen items from the Nueces River by Labonte Park. Police arrested the suspect at his Annaville apartment. He is charged with two counts of burglary. Police said whatever explosives remained in the river did not pose a threat to the public. Officials said the investigation remained active, and that the search would continue as police attempt to recover the remaining items that are missing, including the C4. Source: http://www.kiiitv.com/Global/story.asp?S=13766742

ENERGY

Feds put nation's pipeline operators on notice. Federal safety officials responding to the findings of the San Bruno, Calfornia disaster probe issued a nationwide bulletin January 5 urging operators of natural-gas pipelines to verify they have accurate records about their lines, and to cut pressure on them if they do not. The regulators took the unusual step in response to the discovery that Pacific Gas and Electric Co. had erroneous records about the high-pressure gas line that exploded in San Bruno in September, killing eight people and destroying 38 homes. The revelation raised questions about whether the utility had set the line's maximum allowable operating pressure too high, and whether it had used an inspection method for the pipe that was ill suited to detect some possible weaknesses. The U.S. Pipeline and Hazardous Materials Safety Administration, saying some companies have "failed to detect flaws and deficiencies" in their pipes, called on operators January 5 to do an exhaustive review of records to ensure they are checking for all possible problems. If a pipeline operator cannot make a case for a line's safety, the agency said, it should cut pressure immediately on the line by 20

percent and inspect it. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/01/05/MN001H4F71.DTL

(Hawaii) **Explosion possibly caused by copper theft.** A man was critically injured January 5 after an electrical fuse exploded near the old Hard Rock Cafe in Waikiki, Hawaii. The incident caused a power outage in the area that affected hundreds of customers and the closure of Kapiolani Boulevard, a Hawaiian Electric Co. spokesman said. Witnesses said the transformer fire was near the old Hard Rock Cafe site at the corner of Kapiolani Boulevard and Kalakaua Avenue. They said they could see flames leap up as high as the nearby coconut trees. An injured man ran out onto the street with severe burns, witnesses said. Hawaiian Electric officials said there is evidence the man was trying to steal copper wiring from a locked box with electrical equipment. Source: http://www.kitv.com/r/26379974/detail.html

(Idaho) **BP wind turbines damaged.** In Idaho, the Bonneville County Sheriffs Office is looking for the person or persons responsible for shooting at wind turbines above Ammon causing thousands in damage. A Sheriffs Office spokesman said BP Wind Energy reported that one of their wind turbines was shot twice sometime in the last two weeks. The bullets hit the top of the turbines near the fins and damaged hoses, wiring, and other equipment causing more than $5,000 in damage. British Petroleum Wind Energy says they noticed the damage on December 22 and believe the shooting occurred a few days before that. Vandalism is a felony crime punishable by five years in prison and a fine of $1,000 plus restitution for repairs. Source: http://www.kpvi.com/story.php?id=35035&n=15206

Food and Agriculture

New U.S. food safety law goes into effect. In the biggest overhaul of food safety in the United States since the 1930s, the U.S. President signed a law January 4 giving the Food and Drug Administration (FDA) more power to inspect and shut down food producers. Critics said the changes will have little effect on food-borne infections such as salmonella. New Scientist reports the bill follows an unprecedented series of food poisoning scandals in the United States in recent years, including the recall of half a billion eggs in August 2010 because of Salmonella bacteria, and peanut butter that sickened more than 600 people and may have killed nine in 2009. Source: http://homelandsecuritynewswire.com/new-us-food-safety-law-goes-effect

(Illinois) **Chicago company recalls ground beef.** The Illinois Department of Agriculture said a Chicago company recalled about 200 pounds of ground beef patties because of possible E. coli contamination. The department said January 6 the patties were produced by the Columbus Meat market Inc. December 27, and shipped to food-handling customers in the Chicago area. Each package label on the patties carries the mark “EST. 755” and an identifying date of “12/27/10.” The agriculture department said a sample of the patties tested positive for a strain of E. coli that can cause bloody diarrhea, dehydration, and — in the most severe cases — kidney failure. The company has received no reports of illness linked to the patties. Source: http://www.chicagotribune.com/news/chi-ap-il-beefrecall,0,581784.story

(California) **Customs agents find ‘dangerous’ beetle at LA airport.** U.S. customs officials said January 5 they had intercepted a shipment of rice at Los Angeles International Airport containing a beetle

considered one of the world's most dangerous pests. Agents found live adult and larvae of khapra beetle in a shipment of Indian rice arriving in a shipment of personal effects from Saudi Arabia the week of December 27, a U.S. Customs and Border Protection (CBP) spokesman said in a written statement. Entomologists from the U.S. Department of Agriculture (USDA) said the khapra beetle is one of the world's most destructive pests of grain products and seeds. The CBP spokesman said established infections of the insect were difficult to control because of its ability to live without food for long periods of time, and its relative tolerance to surface insecticides and fumigants. The shipment was quarantined and safeguarded according to USDA guidelines, and destroyed under CBP supervision. Source: http://www.reuters.com/article/idUSLNE70502F20110106

(Maryland) **2 million fish found dead in Maryland.** Authorities in Maryland are investigating the deaths of about 2 million fish in Chesapeake Bay. "Natural causes appear to be the reason," the Maryland Department of the Environment said in a news release. "Cold water stress exacerbated by a large population of the affected species (juvenile spot fish) appears to be the cause of the kill." In Maryland, preliminary tests showed water quality to be acceptable, officials said. "The affected fish are almost exclusively juvenile spot fish, 3 to 6 inches in length," the Maryland department said. A recent survey "showed a very strong population of spot in the bay this year. An increased juvenile population and limited deep water habitat would likely compound the effects of cold water stress." Large winter kills of spot fish have occurred at least twice before in the state, in 1976 and 1980, the department said. Source: http://www.cnn.com/2011/US/01/06/maryland.fish.kill/index.html?hpt=T2

(Connecticut) **Concern over Asian stink bugs.** A lot of Connecticut farmers are worried about Asian stink bugs have turned up in the state. —In certain areas of Eastern Pennsylvania some of the growers down there have lost 50 percent of their crops, the director of the Connecticut Agriculture Experiment Station said. The Asian stink bugs that have turned up apparently hopped rides on cars and trucks from other states. They attack fruits and veggies like a vampire. —The insect has sucking mouth parts, the director said. —So what it does is it will get on a peach, pear or tomato, pepper, it will insert those mouth parts into the fruit, or the vegetable and then it sucks the juices out of that source. Each of those bite marks scabs over with a brown, ugly mark, making the munched on produce unsellable. The state says it may be a year or two before the population grows enough to be a real problem, but they are already drawing up a stink bug battle plan for if and when things get out of hand. Source: http://www.wtnh.com/dpp/news/connecticut/concern-over-asian-stink-bugs

(Wisconsin; Michigan) **More E. coli cases reported from Zillman's smoked meat.** Three new cases of E. coli-related illness have been traced from Michigan back to a Wausau, Wisconsin, butcher shop in which an outbreak first was reported just before Christmas. The illnesses bring to seven the number of people sickened by E. coli-infected smoked meat products produced at Zillman Meat Market in late 2010, the Marathon County Health Department said January 4. The department also expanded its advisory on smoked meats produced at Zillman's to between September 30 and December 23, rather than November 13 and December 23 because the department still has not pinned down the source of the bacteria. While the three cases announced January 4 are new, they are related to the prior four illnesses and involve some of the same people, the Health Department's chronic disease prevention director said. The store has fully complied with the Health Department by thoroughly cleaning the market, and the market remains fully operational. Source: http://www.wausaudailyherald.com/article/20110105/WDH0101/101050600/More-E-coli-cases-reported-from-Zillman-s-smoked-meat

(Oregon) **Invasive medusahead weed threatens ranches in West.** According to a 2010 Oregon State University study, medusahead is rapidly crowding out native grasses, and once established, it eliminates more than 80% of a land's grazing value. Medusahead, native to the Mediterranean area and introduced to the United States in the 1880s, now covers about 1 million acres of Oregon and is spreading across 10 Western states with between 30 million and 76 million acres of public and private land infested, said an Oregon-based scientist with the U.S. Department of Agriculture. —The real risk is how rapidly it's increasing, the scientist said. —The rate is probably doubling every five years right now. Source: http://www.usatoday.com/money/industries/food/2011-01-05-ranchweeds05_ST_N.htm

Historic food safety bill signed into law. The U.S. President signed the long-awaited FDA Food Safety Modernization Act into law January 4. The legislation, widely hailed as the most sweeping update to U.S. food safety law since the Great Depression, survived a constitutional slip-up, repeated filibuster threats, fierce debate over controversial amendments, and managed to advance amidst a jam-packed legislative agenda in one of the most productive Congresses in recent history. In the last 18 months, food safety legislation cleared the Senate twice and the House three times. Source: http://www.foodsafetynews.com/2011/01/historic-food-safety-bill-signed-into-law/

(California; New York) **Chicken mushroom pies recalled by Crave Foods.** Crave Foods, a Los Angeles, California establishment is recalling about 600 pounds of frozen chicken mushroom pies because they contain an undeclared allergen, monosodium glutamate (MSG), which is not declared on the label, the Food Safety and Inspection Service announced January 3. The products subject to recall include: 6-pound cases of "Craves Pies Chicken Mushroom Pie," with each case containing 12 individual packages. The products were produced between September and December of 2010, and were shipped to distribution centers for further retail sales in California and New York. Source: http://www.myhealthnewsdaily.com/chicken-mushroom-pies-recalled-by-crave-foods-0980/

Bumblebee population in US on the decline. Several species of bumblebees in the United States are dying off at a rate researchers are calling "alarming," according to a study published January 3 in the Proceedings of the National Academy of Sciences. In the first large-scale study of the U.S. bumblebee populations, researchers found the populations of four species of agriculturally-important bees have declined by 96 percent, and their range has declined by nearly 87 percent. As with the massive die-offs of honeybees in recent years, the researchers are not certain what forces are at play. The researchers found evidence that, as with honeybees, a pathogen is partly to blame for the drop in numbers. They also believe inbreeding caused by loss of habitat may have a role. Bumblebees, like honeybees, are a key part of growing several crops in North America including tomatoes, blueberries, and cranberries. Bumblebees can pollinate at higher altitudes and in colder weather than other bees. Several studies have been done confirming bumblebees are disappearing also in Europe and Asia. This is the first to confirm their numbers are falling globally. Source: http://www.myfoxdc.com/dpp/news/offbeat/bumblebee-population-in-us-on-the-decline-ncdc-010411

(Alabama) **Alabama firm recalls breaded chicken wing products.** Pilgrim's Pride, a Boaz, Alabama establishment, is recalling approximately 180,000 pounds of breaded chicken wing products because they contain an undeclared allergen, egg, the U.S. Department of Agriculture's (USDA) Food Safety

and Inspection Service announced December 31. Egg is a known allergen, which is not declared on the label. The products subject to recall include: 20-pound boxes of "Pierce Chicken Uncooked Hot & Spicy Breaded Chicken Wings Drummettes and Wing Portions" with the USDA mark of inspection, each box containing four 5-pound bags; 10-pound boxes of "Sweet Georgia Brand Uncooked Hot & Spicy Breaded Chicken Wings 1st and 2nd Sections" with the USDA mark of inspection, each box containing two 5-pound bags. Source: http://www.myhealthnewsdaily.com/alabama-firm-recalls-breaded-chicken-wing-products-0967/

Ground beef sold in N.J. is recalled for possible E. coli contamination. Retailers in six states received shipments of beef products in recent weeks that may contain a deadly strain of the E. coli bacteria, federal officials have said. The organic beef was produced by California-based First Class Foods and sold under several names, according to the U.S. Department of Agriculture. The company is voluntarily recalling 34,373 pounds packaged December 7 and 16. The products were sold under the Nature's Harvest and Organic Harvest brand names. Each of the affected package labels includes the number "EST. 18895" and the identifying pack date "10341 and 10350 Julian date." There were no reports of illness connected to the beef as of December 31, the company said. Concerns about the products were raised after beef produced by First Class on another day tested positive for E. coli O157:H7, a particularly aggressive form of the bacteria, according to federal officials and the company. Source: http://www.nj.com/news/index.ssf/2011/01/ground_beef_sold_in_nj_is_reca.html

(California) **California firm recalls teriyaki beef jerky products.** Bach Cuc Beef Jerky, Inc., a South El Monte, California establishment, is recalling approximately 3,874 pounds of teriyaki beef jerky products because they contain an undeclared allergen, wheat, the U.S. Department of Agriculture's Food Safety and Inspection Service announced December 31. Wheat is a known allergen, which is not declared on the label. The products were distributed to retail establishments nationwide. Source: http://www.myhealthnewsdaily.com/california-firm-recalls-teriyaki-beef-jerky-products-0966/

Companies hope sourcing will stem illegal honey. Honey companies and importers are launching a program in January to try to stop the flow of illegally sourced honey from coming into the United States. The True Source Honey Initiative is an effort by a handful of producers and importers looking to certify the origin and purity of honey sold to U.S. consumers in jars and products such as cereals, snacks, and glazes. Americans consume about 350 million pounds of honey per year, but domestic honey cannot meet that demand. The initiative wants the countries of origin and ingredients inside the honey jar to match the product, said a spokeswoman for Pennsylvania-based Dutch Gold Honey, one of the initiative partners. Certification would come after a third-party annual audit that would cost honey packers and exporters $2,000 to $4,000. The initiative is finalizing a seal it would offer those who pass the audits to place on their packaging. U.S. beekeepers would not be directly subjected to an audit, the spokeswoman said. The U.S. Food and Drug Administration is reviewing a petition seeking a national "pure honey" standard. Source: http://www.dailydemocrat.com/news/ci_16992679

Government Sector (including Schools and Universities)

(Nebraska) **Student kills 1, self at Omaha high school.** The son of a police detective opened fire at a high school in Omaha, Nebraska, January 5, fatally wounding the assistant principal and forcing panicked students to take cover in the kitchen of the building just as they returned from holiday break.The gunman, who had attended the school for no more than 2 months, also wounded the principal before fleeing from the scene and fatally shooting himself in his car. The vice principal died at a hospital hours after the shooting, police said. The principal was listed in stable condition. In a rambling Facebook post filled with expletives, the shooter warned January 5 that people would hear about the "evil" things he did and said the school drove him to violence. He wrote that the Omaha school was worse than his previous one, and that the new city had changed him. He apologized and said he wanted people to remember him for who he was before affecting "the lives of the families I ruined." The post ended with "goodbye." The police chief provided no details on the weapon the gunman used or how he obtained it. The gunman's father is a detective for the Omaha Police Department. Investigators were interviewing the 7-year veteran to try and discern a motive. Source: http://www.usatoday.com/news/nation/2011-01-05-omaha-school-shooting_N.htm

(Georgia) **Unknown white powder at Georgia Southern Univ. taken to Atlanta for further testing.** Public safety officials at Georgia Southern University in Statesboro, Georgia, said preliminary test results came back undetermined on a white powder that was in an envelope mailed to the school. The public safety director at Georgia Southern said the large envelope of "admissions-type papers" actually arrived at Lewis Hall and was opened by an employee January 4, but authorities were not notified until around 9 a.m. January 5. Lewis Hall is home to the GSU Office of Admissions. Statesboro Police and Fire, Bulloch County Sheriff's Office, Georgia Emergency Management Agency, Georgia Bureau of Investigation, FBI, and other agencies from as far away as Swainsboro assisted in the incident. The American Red Cross and Statesboro Fire CAFE Unit also responded with aid. Source: http://www2.wsav.com/news/2011/jan/05/9/update-white-powder-caused-quarantine-ga-southern--ar-1304936/

(Texas) **FBI helping investigate threats in Bay City ISD.** A hand-written death threat letter to Bay City Independent School District in South Texas prompted the parents of hundreds of students to keep their children home. A message January 5 on the school district's website said classes would continue with increased emphasis on safety and security. The FBI and the Texas Department of Public Safety are investigating. Parents on January 3 were advised by the superintendent of the anonymous letter received December 28. The letter written to the superintendent contains profanity, misspellings, and refers to the sender's child getting in trouble. The sender included new —rules on discipline and threatened to —kill a random student if the demands were not met. About half the students in the nearly 3,800-student district missed school January 4. Source: http://www.chron.com/disp/story.mpl/ap/tx/7366576.html

(Tennessee) **Bomb threat in county building.** A bomb threat briefly emptied the Robertson County, Tennessee, office building just before 2 p.m. January 4. The Robertson County 911 Center was advised by Sumner County that they had received the threat from an untraceable cell phone number, and that the link was traced to a cell tower in Sumner County. The caller said the bomb was in

General Sessions Court in Robertson County. A captain at Robertson County Sheriff's Office had the building sealed and searched before allowing people back in. The search was done quickly and efficiently, and it turned up no indication of explosives. Once the building was declared safe, people filed back in to offices and courtrooms to resume schedules that had been interrupted. Source: http://www.tennessean.com/article/20110104/ROBERTSON01/110104048/Bomb-threat-in-county-building

(Pennsylvania) **Bomb threat prompts scare at city hall.** A man who called 911 and threatened to blow up the Bethlehem Police Department in Bethlehem, Pennsylvania prompted a scare in and around city hall, police said. The call was received at approximately 10 a.m. January 3. Police said the man told the call-taker there was already someone with a bomb in front of city hall, which was immediately locked down. Police diverted traffic away from city hall as officers and firefighters searched the area. An unattended package was found on the west side of the city hall complex, but it was deemed harmless and unrelated to the bomb threat. Police gave the all-clear around 11:15 a.m., but then another suspicious package was found next to the library. The library was then evacuated and surrounding streets were closed again. Source: http://www.wfmz.com/lehighvalleynews/26351982/detail.html

(Illinois) **Hackers shut down state website.** Unknown hackers shut down an Illinois state Web site for several hours January 2 and 3. The Illinois Senate Democrats site — senatedem.ilga(dot)gov — appeared simply as a blank white screen with the words, "by 3n_byt3 @ indonesia hackers :P" in the center from the evening of January 2 until 8 a.m. January 3, when the site was repaired. The communication director for the Illinois Senate Democrats said there were a number of attempts to hack the site, but he did not know who was responsible. A Webmaster added hackers were able to exploit a weakness in the Windows operating system, and said staffers were working on resolving the issue. Source: http://www.pantagraph.com/news/state-and-regional/illinois/article_ab3ba49a-17ae-11e0-9eca-001cc4c002e0.html

Malware campaign cyber-espionage or cyber-crime? The crew behind the Kneber botnet that made headlines in 2010 may have surfaced again in a malware campaign targeting employees of various governments. The botnet, which pushes out the Zeus Trojan, was spotted around Christmas time spamming out malware through a phony holiday message from the White House. Those who received the card and either clicked on a link to an e-card or opened a malicious attachment were compromised. The fact Zeus was stealing data will come as no surprise to anyone familiar with the Trojan; but the idea that a piece of malware most commonly associated with swiping banking credentials was after documents raised some eyebrows. According to a security blogger, the botnet operators were able to get their hands on more than 2 gigabytes of PDFs, Microsoft Word, and Excel documents from dozens of victims, including an employee at the U.S. National Science Foundation's Office of Cyberinfrastructure and an official with the Moroccan government's Ministry of Industry, Commerce, and New Technologies. Source: http://www.eweek.com/c/a/Security/Malware-Campaign-Cyber-Espionage-or-Cybercrime-626011/

(California) **Bomb threat called in at high school.** A bomb threat called from a pay phone January 3 prompted sheriff's officials to send the bomb squad to San Clemente High School in San Clemente, California, where classes were expected to resume the same day. Members of the Orange County Sheriff Department's bomb squad, as well as bomb-sniffing dogs, searched the school for nearly 4

hours, but found no dangerous material, said a police lieutenant with the sheriff's department. Deputies received a call at 1:30 a.m. of a possible bomb inside the school. Source: http://www.ocregister.com/news/bomb-282461-school-england.html

Policy puts troops at risk for identity theft. U.S. troops may be among the most vulnerable Americans to identity theft. That is because the U.S. military is overusing Social Security numbers (SSNs) and putting at risk troops' most basic personal information, according to a report from several professors at the U.S. Military Academy at West Point in New York. The problem has been apparent for years, and the Pentagon has issued a stream of policies and directives to curtail the risk. But the underlying problem is a culture where troops are constantly prompted to provide their SSNs when doing basic daily tasks such as logging onto computers, signing up for medical care, and accessing routine military facilities. "The military culture is one of widespread compulsory Social Security number disclosure," concluded the report, released in early December and published online by the Small Wars Journal. "We need widespread, systemic changes to the culture and processes surrounding the use of personal information, and these changes need to be embraced and enforced by commanders at every level," the report said. Source: http://www.armytimes.com/news/2011/01/military-troops-at-risk-for-identity-theft-010211w/

(District of Columbia; Virginia) **Airspace breach shuts Capitol.** The U.S. Capitol complex in Washington D.C. was evacuated January 1 when an aircraft entered restricted space, prompting a 30-minute shutdown of the Senate and House buildings. Capitol Police contacted the pilot of the errant aircraft, which landed safely at Ronald Reagan Washington National Airport in Arlington, Virginia. Capitol Police and the Transportation Security Administration are investigating the incident. Much of the Capitol complex was empty because lawmakers and staffers were away for the holidays. Source: http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102473.html

(Florida) **Library bomb threat brought Levy County police dog to Gainesville.** A Levy County Deputy and his K-9 partner, who is trained to sniff bombs, were needed to search the Alachua County Library in Gainesville, Florida, after a bomb threat was called in December 30. Because of the size of the library — 86,000 square feet — Gainesville police needed extra help to search. "It was a bomb threat and with all of that space it would have been a safety issue and would have taken forever [to search] without that dog," a Gainesville police corporal said. "Levy County was the closest one that they could get to at the time." A bomb-sniffing team from the Alachua County Sheriff's Office was able to join the search later. No bomb was found. Source: http://www.gainesville.com/article/20110101/COLUMNISTS/110109995/1020/news?Title=Library-bomb-threat-brought-Levy-County-police-dog-to-Gainesville&tc=ar

(Texas) **Lubbock prisoner claimed Al Qaeda ties, threatened President.** A one-time prisoner at the Montford prison unit in Lubbock, Texas, admits he claimed to be part of Al Qaeda and that he threatened to kill the U.S. President. The 37-year-old admitted he wrote letters in 2009 to government officials that said he would blow up government workers. According to court records, another letter said, "In the name of Allah down with the USA and down with the President of the USA. I will get out soon and when I do I will kill your President." As part of a guilty plea, those letters will cost the man up to 15 years in prison. Source: http://www.kcbd.com/Global/story.asp?S=13765696

Information Technology and Telecommunications

Apple's Mac App Store hacked on first day. Apple's launch of the new Mac App Store January 6 has already been marred with reports of hackers coming up with ways to pirate paid apps on the platform. Hackers have discovered a simple copy-paste method to illegally crack some of the paid apps on store. The method involves replacing the receipt and signature files on a paid app package with ones taken from a free app. According to Apple Insider, Apple provided support for App Store receipts on Mac OS X 10.6.6, but it is clear Apple failed to check the Mac App Store for vulnerabilities like this before launching it. A report on technology blog Daring Fireball said the vulnerability only affects those apps which do not follow Apple's app validation advice, in which the application is required to check for a valid receipt along with making sure that the receipt matches the app's bundle ID. Source: http://www.itproportal.com/2011/01/07/apples-mac-app-store-hacked-first-day/

Survey scammers and adware pushers target TRON fans. Security researchers warn of multiple scams that trick fans of the "TRON" movie into subscribing to premium rate services or infecting their computers with adware. Most of the scams offer to view the movie online at high quality. These are usually advertised through YouTube videos with titles among the lines of "Watch TRON : Legacy Online HD Blu-Ray Quality." Clicking on the links listed in the descriptions of these videos leads users to Web sites that ask them to take a survey before being given access to the movie. These deceptive surveys usually attempt to subscribe users to premium rate services and collect their personal information for future targeted spamming in the process. Other TRON free streaming scams use the "required codec" social engineering trick to get users to download and install Adware programs like ClickPotato, ShopperReports, QuestBrowser, and blinkx Beat. Source: http://news.softpedia.com/news/Survey-Scams-and-Adware-Pushers-Target-TRON-Fans-176321.shtml

The hidden risks of social media. Europol's new Internet facilitated organized crime (iOCTA) report examines how European Union citizens are risking their personal identities, privacy, and computer data through the use of social media tools which are increasingly a target for cybercriminal activity. In recent years the transition of the world wide web from a collection of websites to a platform for linked services such as social networking sites and real–time communication tools (_Web 2.0'), has provided the technical means for the expansion of social engineering. Cybercriminals exploit the trust of users — who consider themselves to be in a _safe' network of people they know — by injecting malicious software into posted items and sharing links to websites that are bogus and designed to extract personal information. The majority of organizations have come to accept the use of social networking sites in the workplace. But under the right circumstances, access to social media at work has the potential to infect corporate networks with spyware and other means to harvest large amounts of personal, corporate, and financial data for profit. Source: http://www.europol.europa.eu/index.asp?page=news&news=pr110105.htm

Floating point DoS attack. A bug in the way the PHP scripting language converts certain numbers may cause it to tie up all system resources. For example, on 32-bit systems, converting the string —2.2250738585072011e-308 into a floating point number using the function zend_strtod results in an infinite loop and consequent full utilisation of CPU resources. PHP 5.2 and 5.3 are affected, but apparently only on Intel CPUs which use x87 instructions to process floating point numbers. The x87 design has long been known to contains a bug which triggers just this problemPDF when computing

approximations to 64-bit floating point numbers. By default, 64-bit systems instead use the SSE instruction set extension, under which the error does not occur. Processing the numbers 0.22250738585072011e-307, 22.250738585072011e-309 and 22250738585072011e-324 also triggers an infinite loop. It may also be possible to remotely disable some server systems merely by sending this value as a parameter in a GET request. The PHP development team has fixed this in the forthcoming version 5.3.5. A patch for version 5.2.16 is available from the repository. Source: http://www.h-online.com/security/news/item/Floating-point-DoS-attack-1163838.html

Recent spam campaign points to new Storm botnet. While analyzing a recent spam campaign, security researchers found what seems to be a new version of the Storm or Waledac botnets. According to the Shadowserver Foundation, a recent junk e-mail campaign distributed links that led to a new Waledac or Storm variant. The e-mails come with a subject announcing a holiday e-card, while their body message direct users to links to view the alleged greeting. These links lead to HTML pages hosted on compromised Web sites, which in turn execute a meta redirect towards one of multiple domain names controlled by the attackers. The domains are using fast flux hosting — they respond to multiple IP addresses and are difficult to shut down. The landing pages on these domains display a message reading "Can't view the greeting? Download Flash Player!" If the visitor does not click on the link to download the alleged Flash Player installer within 5 seconds they are redirected to a secondary page which serves several exploits for outdated software installed on their computer. If they do click on the link, a file called install_flash_player.exe is downloaded. If executed, this file opens an Internet Explorer connection to the same exploit page. In both scenarios, successful exploitation downloads the new Storm variant. Source: http://news.softpedia.com/news/Recent-Spam-Campaign-Suggest-New-Storm-Botnet-175866.shtml

Chinese hackers dig into new IE bug, says Google researcher. An accidental leak may have confirmed Chinese hackers' suspicions that Internet Explorer has a critical unpatched vulnerability, a security researcher said January 1. The bug was one of about 100 found by a noted browser vulnerability researcher and Google security engineer using a new "fuzzing" tool. The vulnerabilities were in IE, Firefox, Chrome, Safari, and Opera. According to the researcher's account, a developer working on WebKit — the open-source browser engine that powers Apple's Safari and Google's Chrome — "accidentally leaked" the location of the then-unreleased fuzzing tool. Google's search engine then added that location to its index. "On December 30, I received ... search queries from an IP address in China, which matched keywords mentioned in one of the indexed cross_fuzz files," the researcher said. Those searches were looking for information on a pair of functions in "Mshtml.dll," IE's browser engine, that he said were unique to the vulnerability, and that had "absolutely no other mentions on the Internet at that time." The person or persons searching for the functions then downloaded all the available cross_fuzz files. Source: http://www.computerworld.com/s/article/9202959/Chinese_hackers_dig_into_new_IE_bug_says_Google_researcher

27C3: danger lurks in PDF documents. At the 27th Chaos Communication Congress (27C3) in Berlin, Germany a security researcher from the U.S. company FireEye noted security problems in connection with Adobe's PDF standard. A PDF can reportedly contain a database scanner that becomes active and scans a network when the document is printed on a network printer. Also, it is reportedly possible to write PDFs that display different content in different operating systems, browsers, or PDF readers – or even depending on a computer's language settings. The researcher said other risks are

generated through the support of inherently insecure script languages such as JavaScript, formats such as XML, RFID tags and digital rights management (DRM) technologies. Source: http://www.h-online.com/security/news/item/27C3-danger-lurks-in-PDF-documents-1162166.html

National Monuments and Icons

(California) **Mysterious tar balls on beach.** Tar balls that turned up on Limantour Beach at Point Reyes, California are being analyzed to determine where they came from. Hundreds of the ping-pong-sized balls were found on the beach at the beginning of last week by volunteers from the Gulf of the Farrallones Marine Sanctuary's Beach Watch program. "It was along a two-mile stretch of the beach, but we are not quite sure what the source is," a marine sanctuary spokeswoman said. Other area beaches also had the tar balls, but not as many as seen at Limantour, she said. Storms and high tides have since washed the mess away. For a time, the area saw numerous tar balls wash up on beaches. Those were created by oil that leaked from the S.S. Jacob Luckenbach. The freighter sank in 1953 about 17 miles southwest of the Golden Gate Bridge, but was not identified as the source of the material until 2002 after decades of leaking oil, especially during winter storms, causing injury to wildlife. In 2002, the U.S. Coast Guard oversaw a $19 million effort to remove oil from the Luckenbach and to seal it to prevent further oil releases. Source: http://www.marinij.com/westmarin/ci_17017771?source=most_viewed

(Alaska) **High avalanche danger.** Avalanche danger has increased to high level on all windloaded slopes greater than 30 degrees in the Turnagain Arm and Turnagain Pass areas of Alaska January 3, according to a spokeswoman with the Chugach National Forest Avalanche Information Center. Non-affected slopes and rain-saturated terrain at the lower elevations pose considerable danger. Large natural and human-triggered avalanches are likely, with up to 18 inches of new snow, hurricane-force winds and heavy rains at lower elevations. After the weather improves, natural avalanches will subside, but most steep slopes at the mid and upper elevations will be hair-trigger for the next 24 hours, she said. Source: http://thesewardphoenixlog.com/article/1101high_avalanche_danger

(California) **Yosemite road closures clear after rock slide.** The rock slide that closed the Highway 140 route into Yosemite National Park in California December 30 was reopened the evening of December 31, but rangers advised checking road conditions before starting out. All roads around the park, except for the seasonal closures of Tioga and Glacier Point roads, remained open, park officials said January 1. Visitors were urged to be aware of tire-chain requirements while traveling through Yosemite. The rocks fell half a mile east of Yosemite View Lodge in El Portal, just inside the park boundary. Park officials said the boulder is 10 to 15 feet high, 6 feet wide and 4 feet deep. Routes from Fresno on Highway 41 and through Big Oak Flat and Groveland on Highway 120 were open, but travelers should bring chains, a park ranger said. There were about 8 inches of snow on the valley floor December 31, and another inch was forecast for January 1, she said. Source: http://www.modbee.com/2010/12/31/1492945/yosemite-road-closures-clear-after.html

Postal and Shipping

(Maryland) **2 fiery packages put Maryland mailrooms on alert.** A disgruntled "lone wolf" griping about highway signs mailed a small package to Maryland's Democratic governor and the parcel

ignited when someone in the state mailroom unzipped it, shooting out a tiny flame that singed the worker's fingers. About 15 minutes later January 6, a second worker was injured opening a similar package at a state government building 20 miles away. Soon after, mailrooms across Maryland were cleared and two other suspicious packages uncovered, though they turned out to be a toner cartridge and laptop batteries. Explosive material was not found in either package that ignited and authorities are not sure if any other dangerous packages are out there, but mailroom workers were expected back at work January 7. They will have pictures of the packages and were advised to be vigilant about anything suspicious. Meanwhile, the packages have prompted officials in at least four nearby states to be more vigilant. Source: http://www.9wsyr.com/news/local/story/2-fiery-packages-put-Maryland-mailrooms-on-alert/ErBr3mMywUaqlN0zO4r5PQ.cspx

(Texas; Colorado) **Anthrax hoax shuts down UPS station overnight.** Authorities responded to an anthrax threat in a United Parcel Service (UPS) package about 7 p.m. January 6 that turned out to be a hoax, Corpus Christi, Texas police said. An active duty Army Iraq War veteran stationed at Fort Collins, Colorado, sent a 3-foot by 3-foot package weighing about 19 pounds to his former mother-in-law after sending her a text he was shipping Anthrax to her and her daughter, his ex-wife, a police captain said. The soldier also is suspected of having some post war trauma problems, he said. The Corpus Christi Fire Department's hazardous materials team was the first to handle the package, after police closed access to the UPS terminal in the 300 block of Navigation Boulevard. The street was closed for about 3 hours between Agnes and Leopard streets as a precaution, the spokesperson said. The soldier has been identified, and could face federal charges, which will be handled by the FBI. Source: http://www.caller.com/news/2011/jan/07/anthrax-hoax-shuts-down-ups-station-overnight/

US to launch new effort to bolster cargo security. The Homeland Security Secretary said the United States is launching an effort to improve cargo security and protect infrastructure and supply networks worldwide. She said the European Union and other international organizations will participate. She did not elaborate, saying only the Global Shield program would be tightened to prevent transport of bomb–making chemicals. The intelligence–sharing program launched by Homeland Security and 60 other nations last year has reportedly intercepted a number of suspicious shipments worldwide. Source: http://topnews360.tmcnet.com/topics/associated-press/articles/2011/01/06/132118-us-launch-new-effort-bolster-cargo-security.htm

The influence game: Safety, trade interests clash. A Presidential Administration proposal aimed at preventing air shipments of lithium batteries from causing fires in flight is drawing fierce opposition from some of the United States' top trading partners, who say it would disrupt international shipping and drive up the cost of countless products. The European Union, China, Japan, South Korea, and Israel are lobbying against requiring air shipments of lithium batteries and products containing them to meet hazardous cargo regulations, diplomatic and industry officials told the Associated Press. At a minimum the proposal could cost hundreds of millions of dollars and disrupt the flow of products such as cellphones, laptops, medical devices, water meters, and electric car batteries, among others, these governments say. But the Transportation Department estimates its proposal would cost only $9 million per year. Pilot unions want the additional safety precautions, saying it is only a matter of time before the batteries cause a plane crash. Source: http://www.washingtonpost.com/wp-dyn/content/article/2011/01/03/AR2011010300564.html

(New Jersey) **Four Newark council members receive threatening notes laced with baking powder.** Four Newark, New Jersey council members have received threatening letters laced with a white powder in an apparent hoax that has unnerved city leaders, authorities said December 30. Investigators would not disclose what the letters said but confirmed the substance was only baking soda. While the city's emergency services descended on city hall to investigate December 30, it was business as usual for the council, which conducted a scheduled meeting. Members were given a security briefing afterward. The incident is being investigated by the Newark Fire Department and its hazardous-materials team. Source: http://www.nj.com/news/index.ssf/2010/12/four_newark_council_members_re.html

PUBLIC HEALTH

(New Mexico) **Suspect named in New Mexico hospital shooting.** A suspect fired his gun inside the University of New Mexico Hospital in Albuquerque, New Mexico, January 4, but no one was injured, the university and police said. Police identified the apparent gunman as a 21-year-old man. Witnesses told officers that a female patient was with her child when the woman's boyfriend entered the room, police said. The couple began to argue. During the altercation, the suspect pulled out a small handgun and purposefully fired it, according to a statement from the Albuquerque Police Department. Source: http://articles.cnn.com/2011-01-04/justice/new.mexico.hospital.gunman_1_apparent-gunman-new-mexico-hospital-lockdown-order?_s=PM:CRIME

Recall of AngioSculpt PTA scoring balloon catheters. AngioSculpt percutaneous transluminal angioplasty (PTA) scoring balloon catheters, manufactured by AngioScore Inc, are subject to a class I U.S. Food and Drug Administration (FDA) recall because of retained device fragments or significant arterial injury, which may lead to death or the need for additional surgical intervention. The FDA issued the safety alert from the MedWatch FDA Safety Information and Adverse Event Reporting Program January 5. The recall affects 17,682 AngioSculpt PTA scoring balloon catheters (OTW 0.018" Platform) of multiple sizes, including all sizes and lot codes for the following models: 2076-4020, 2076-5020, 2076-6020, 2092-6020, and 2105-6020. Products were manufactured by AngioScore, Inc, from September 2009 to November 2010. A Medical Device Recall notification letter dated November 15, 2010, was issued to U.S. customers, who were instructed to immediately discontinue distributing and using any affected product. Source: http://www.medscape.com/viewarticle/735355

Myriad flu strains emerging worldwide. As confirmed cases of influenza in the United Kingdom over the last couple of weeks rose from 40 percent to 50 percent and at a level that qualifies as an epidemic, flu virus strains also have begun to spread elsewhere in Western Europe, the Middle East, and Southeast Asia. In the United States, the Centers for Disease Control and Prevention (CDC) reported that flu activity is now rampant in New York, Alabama, Georgia, and Mississippi. Moderate flu infections have been reported in Louisiana, Arizona, Florida, Illinois, Kentucky, and Nevada. —The District of Columbia and 48 states from all ten surveillance regions have reported laboratory-confirmed influenza this season, CDC stated, adding that —while activity in other areas of the country is increasing, Region 4 in the Southeastern United States has accounted for 2,664 (54.8 percent) of all 4,864 reported influenza viruses this season, including 1,547 (78.9 percent) of the 1,961 influenza B viruses. Disturbingly, CDC noted that —high levels of resistance to the [antivirals] amantadine and rimantadine persist among 2009 influenza A H1N1 and A H3N2 viruses, emphasizing that —the adamantanes are not effective against influenza B viruses circulating globally. Source:

http://www.hstoday.us/briefings/daily-news-briefings/single-article/myriad-flu-strains-emerging-worldwide/130e079705c2f7f70accd6bff45633b5.html

(Massachusetts) **Armed, intoxicated Cambridge man forces evacuation of hospital.** A floor at McLean Hospital in Belmont, Massachusetts, was evacuated December 29 after an armed and intoxicated Cambridge man allegedly verbally abused the staff and refused to leave the hospital. According to a police report, the 60-year-old man entered one of the hospital buildings wearing a holstered handgun underneath his coat and became verbally abusive to McLean staff when asked about the gun. He then reportedly went into a room to visit a female patient he knew. Belmont police were called to the scene and evacuated the floor while officers engaged in limited conversation with the man through the closed door of the woman's room. The North Eastern Massachusetts Law Enforcement Council SWAT team was also called to the scene. As the SWAT team arrived and suited up, the man allegedly exited the room, unholstered his pistol and pointed it in the direction of the Belmont officers surrounding the room. The suspect was ordered to drop his weapon, which he did. He was then taken into custody without further incident. The man was arrested and charged with assault by means of a dangerous weapon and carrying a firearm while under the influence of alcohol. Source: http://www.wickedlocal.com/cambridge/news/x1458581999/Armed-intoxicated-Cambridge-man-forces-evacuation-of-hospital

(Maryland) **Employee attacked, killed inside Maryland hospital.** An employee was attacked and killed inside a Bethesda, Maryland hospital January 1, forcing the facility to lock down for several hours while police searched for an assailant. The 40-year-old worker was assaulted in a non-patient care area of Suburban Hospital at about 10:30 a.m., a spokeswoman said. The hospital was locked down for several hours, and no one was allowed to leave, while police conducted a thorough search of the hospital and grounds. "Patients, staff and visitors were safe throughout the ordeal and kept apprised of the situation via personnel in a command center established at the hospital in case of an event or disaster," she said. The hospital was reopened at about 2:25 p.m. local time. A Montgomery County Police spokeswoman said the assailant was not found during the search and that the case was being treated as a homicide. Source: http://www.reuters.com/article/idUSTRE7001GY20110101

(Texas) **Security device prompts bomb squad call, evacuation.** A business owner's homemade security device inside an office in the South Texas Medical Center caused a security guard to call 911 to report the suspicious device, resulting in a fire and police response that closed a nearby McDonald's and cordoned off several businesses January 2. A San Antonio, Texas police sergeant said the owner of Argus Environmental Consultants, who was in Atlanta but reached by telephone January 2, told police he had wired a propane tank with an electronic device and a note to the inside of the office's front door to deter burglars. The note read, "If this detonates, call 911," he said. Police and fire officials took the device seriously when the security guard called around 6:15 a.m., cordoning off other offices and businesses within 300 feet. The hazardous materials team, bomb squad, and arson investigators assisted in the investigation, along with several police officers, firefighters, and medical officials. Source: http://www.mysanantonio.com/news/local_news/article/Security-device-prompts-bomb-squad-call-932495.php

Transportation

Napolitano: Israeli-style security won't work for U.S. The Homeland Security Secretary January 4 rebuffed suggestions that U.S. airports should adopt the practices of airports in Israel, calling the Israeli air travel system —a very different model. —We share a common goal, which is to protect the people of our countries from terror or other attacks, she told Fox News ahead of a tour of security facilities at Tel Aviv's Ben-Gurion International Airport. But there are many differences in the United States system versus Israel. Part of that is driven by sheer size. Critics of U.S. security methods, particularly full body scans and the so-called —invasive pat down used by the Transportation Security Administration, have called for American airports to adopt Israeli-style security measures, which rely heavily on behavioral profiling of travelers. But the Secretary said that what is effective in Israel, a nation of 7.3 million, would not necessarily work for 310 million Americans. Ben-Gurion is Israel's only major international airport. The United States, however, has 450 such facilities. Plus, about 11 million people pass through Israeli airports each year, while 70 times that many passengers go through American airports each year. January 4, the head of security at Ben-Gurion gave the Secretary a tour of his airport's system and a —comprehensive briefing on Israeli airport security that —covered the spectrum from intelligence to the perimeter security of the airport to checkpoint screening and everything in between, according to a Homeland Security official. Source: http://www.foxnews.com/politics/2011/01/04/napolitano-israeli-style-security-wont-work/

(New York) **Brooklyn bus depot in terror scare over mysterious filming of gas tanks.** Terror fears have struck a Brooklyn, New York bus depot after reports that several suspicious people videotaped its highly-flammable natural gas tanks. —If those were hit, the whole neighborhood would blow up, said a Transport Workers Union representative who responded to the reports. Three incidents of mysterious filming were reported on January 1-3 at the Jackie Gleason bus depot in Sunset Park. Police say they are investigating. Those who spotted the individuals described them as —Middle Eastern'' looking, and said they paid particular attention to the depot's compressed natural gas tanks, near its front gate. Only one guard is usually on duty at the depot, said sources. Early January 1, a man dressed in a business suit walked by the depot with a video camera, transit sources said. January 2, two men and a woman allegedly parked their gray BMW with Pennsylvania plates in front of the depot, and filmed it with a large video camera. The mysterious videographers waited for the guard to take a bathroom break before shooting their footage, said the sources. January 3, another man was spotted filming buses along their routes in the neighborhood. Union officials also found the gate to a separate entrance to the bus depot wide open yesterday, with no guard in sight. Four MTA counter terrorism officers were at the depot reviewing security footage of the incidents January 4. Source: http://www.nypost.com/p/news/local/brooklyn/terror_fear_at_klyn_bus_depot_zaPgJhWuo8tobuJHGl1LjK

Water and Dams

Wastewater treatment lowers pathogen levels. A recent study by a team of researchers at the University of Arizona has tracked the incident of pathogens in biosolids over a 19-year period in one major U.S. city. In the same study, the researchers also analyzed pathogen levels in biosolids at 18 wastewater treatment plants in the United States. Their analysis indicates pathogens levels have

dropped since the implementation of federal regulations on treating sewage in 1993. These treatment guidelines have proven to be extremely effective with 94 percent to 99 percent of all pathogens in biosolids eliminated after wastewater treatment. The term biosolid refers to sewage sludge that has undergone a certain level of treatment and is divided into two classifications. Class A biosolids undergo a high level treatment and do not show any signs of pathogens. In contrast, Class B biosolids receive a lower amount of treatment and have been found to contain bacterial, parasitic, and viral pathogens. Around 5.5 billion kilograms of biosolids are produced annually in the United States, with the vast majority being Class B. Approximately 60 percent of the annual production of biosolids is used as agricultural fertilizer. Source: http://www.eurekalert.org/pub_releases/2011-01/asoa-wtl010311.php

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**